International Journal of Theoretical Physics, Vol. 39, No. 3, 2000

Quantum Nondeterministic Computation[†]

Giuseppe Castagnoli[1] and Dalida Monti[1]

Received December 8, 1999

We investigate the possible contribution of quantum measurement in yielding the quantum computation speedup appearing in a modified version of Simon's algorithm.

Growing attention is being given to whether quantum algorithms follow a common pattern (Cleve *et al.*, 1997, among others) and the reason for the quantum computation speedup with respect to Turning machine computation (Ekert and Jozsa, 1998, among others). We shall apply the following interpretation to Simon's algorithm: quantum computation speedup comes from the fact that the evolution of a quantum system undergoing measurement is affected by both the initial actions (i.e., by the preparation of the initial state and the subsequent unitary transformations) and by the need to satisfy some logical-mathematical constraints set by the final action of measurement. The most conspicuous constraint is that the outcome of a measurement is a *single* eigenvalue/eigenstate of the measurement basis. These constraints are partly or completely irrespective of the initial actions, and therefore the computation process is affected in a nonredundant way by both the initial actions and the final measurement action; in this sense we mean it is nondeterministic.[2]

In the interpretation we are going to propound, measurement is not only needed to read the solution of the problem (or something useful to frame the solution). Quite the contrary, *together* with the reversible initial actions, measurement creates the solution in such a way that there is a computational speedup. As a matter of fact, given a suitable preparation, the final measure-

[†] This paper is dedicated to the memory of Prof. Gottfried T. Rüttimann.

[1] Elsag Bailey and Università di Genova, 16154 Genova, Italy.

[2] In our interpretation, the quantum computation speedup is treated with the notion, due to Finkelstein (1996), that there are only initial and final actions, with "quantum spontaneity" (originated by measurement) in between.

0020-7748/00/0300-0525$18.00/0

ment action can be seen as an analog form of computation which, at the same time, introduces and satisfies a system of simultaneous Boolean equations representing the problem to be solved, or the hard part thereof.

To show this, we consider a quantum system made of two n-qubit registers a and v (a for *argument*, v for *value* of a function of that argument). Given $B^n = \{0, 1\}^n$, $N = 2^n$, let $\mathcal{H}_{av} = \text{span}\{|x\rangle_a\ |y\rangle_v\}$, with (x, y) running over $B^n \times B^n$, be the Hilbert space of the two registers, and

$$|\varphi, t_2\rangle_{av} = \frac{1}{\sqrt{N}} \sum_x |x\rangle_a |f(x)\rangle_v \tag{1}$$

be the quantum state before measurement, say at time t_2 (subscripts will refer to Fig. 1a; see below). Here φ labels the ket, x runs over $0, 1, \ldots, N - 1$, and $f(x)$ is a function from B^n to B^n. We designate the binary number stored in register a (v), a Hermitian operator, by $[a]$ ($[v]$).

Measuring $[v]$ in state (1) yields some specific eigenvalue $\bar{f} \in \{f\}$, where $\{f\}$ is the set of the eigenvalues for the measurement basis, which must cover the values assumed by $f(x)$. Correspondingly, the state of the quantum system changes to

$$|\beta, t_3\rangle_{av} = \bar{k} \sum_x |x\rangle_a |\bar{f}\rangle_v \tag{2}$$

where x runs over all x such that $f(x) = \bar{f}$ and $\bar{k} = |\bar{k}|e^{i\delta}$ are a normalization and a random phase factor (the latter will be understood from now on). Although we are dealing with the evolution of the same quantum system, we have changed labels from φ to β to emphasize that $|\beta, t_3\rangle_{av}$ is not univocally determined by $|\varphi, t_2\rangle_{av}$, for it is also influenced by the final measurement action. In a problem-solving context, it is easy to see that there is more than a random influence. This is best shown by using a special (algebraic) representation of the usual description of quantum measurement, such that the *result* of measurement becomes the *solution* of a system of simultaneous equations applying to a ket variable belonging to the Hilbert space $\mathcal{H}_{av}$. This ket variable, in elementary algebra, would be called the "unknown" of the system of simultaneous equations.

Let us designate by $|\psi\rangle_{av}$ this ket variable, which is only constrained by normalization, thus: $|\psi\rangle_{av} = \Sigma_{x,y}\ \alpha_{xy}|x\rangle_a|y\rangle_v$, where (x, y) runs over $B^n \times B^n$ and α_{xy} are complex variables independent of each other up to $\Sigma_{x,y}\ |\alpha_{xy}|^2 = 1$. There are three equations, to be simultaneously applied to $|\psi\rangle_{av}$, whose solution is the measurement outcome $|\beta, t_3\rangle_{av}$.

(i) The measurement outcome must be a *single value*, namely any eigenvalue of the measurement basis. This constraint is represented by the projection equation

$$P_v|\psi\rangle_{av} = |\psi\rangle_{av}, \qquad \text{where} \quad P_v = |f\rangle_v\langle f|_v, \quad f \in \{f\} \tag{3}$$

$|\psi\rangle_{av}$ satisfying Eq. (3) is a ket variable belonging to the Hilbert subspace $\mathcal{H}^f_{av} = \text{span}\{|x\rangle_a|f\rangle_v\}$, with x running over B^n and f being fixed. The number of such subspaces is, of course, the number of the eigenvalues. It may be convenient to think of the action of measurement as an analog form of computation that we can choose to exploit; a significant logical constraint, to be satisfied by the measurement outcome, is introduced by this very choice. This is of course a universal constraint, holding for any initial actions, therefore *independent* of the initial actions.

(ii) Provided that constraint (3) is satisfied, the inner product

$$|\langle\psi|_{av}|\varphi, t_2\rangle_{av}| \quad \text{must be maximum} \tag{4}$$

$|\psi\rangle_{av}$, belonging to $\mathcal{H}^f_{av}$, and satisfying (4), becomes the projection of $|\varphi, t_2\rangle_{av}$ on $\mathcal{H}^f_{av}$. Together, (3) and (4) yield $|\psi\rangle_{av} = k|f\rangle_v\langle f|_v|\varphi, t_2\rangle_{av}$, $f \in \{f\}$, where k, depending on f, is a normalization factor. The operator $|f\rangle_v\langle f|_v$, to be applied to $|\varphi, t_2\rangle_{av}$, is independent of the initial actions. It selects, out of the superposition $|\varphi, t_2\rangle_{av}$, all and only those tensor products containing $|f\rangle_v$, which naturally survive in the measurement outcome.

(iii) The result of measuring $[v]$ must be a specific value:

$$f = \bar{f} \tag{5}$$

where $\bar{f}$ is randomly chosen among the values of f (x) appearing in $|\varphi, t_2\rangle_{av}$ according to probability amplitudes. $\bar{f}$ is *partly* independent of $|\varphi, t_2\rangle_{av}$, for it is stochastically related to it. We should note that only Eq. (5) is represented in the usual statement that the measurement outcome is random, whereas Eq. (3) and (4) are not.

The solution of the system of simultaneous equations (3)–(5) is $|\psi\rangle_{av} = \bar{k}|\bar{f}\rangle_v\langle\bar{f}|_v|\varphi, t_2\rangle_{av} = |\beta, t_3\rangle_{av}$, indeed the state after measurement of the quantum system [Eq. (2)].

This shows that the outcome of the computation process is determined by both the result of the initial actions $|\varphi, t_2\rangle_{av}$ and the requirement of satisfying a system of simultaneous constraints that are introduced by the final measurement action and are partly independent of $|\varphi, t_2\rangle_{av}$. Of course, this dual effect cannot apply to a classical evolution. Being (in principle) completely determined by an initial condition, such an evolution cannot satisfy a final constraint independent of it. We will show how this dual influence can justify Simon algorithm computational speedup. The scheme is that, by properly representing the problem to be solved in the state-before-measurement, Eqs. (3)–(5) become a system of simultaneous Boolean equations customized on such a problem. Measurement, by both introducing and

solving this system, produces the solution of the computationally hard part of the problem.

We shall outline a modified version (Cleve *et al.*, 1997) of Simon's algorithm (Simon, 1994). Given a 2-to-1 function $f: B^n \to B^n$ such that $\forall x > x'$: $f(x) = f(x') \to x = x' + r$ for some $r \in B^n$, and hard to reverse by known classical means, the problem is to find r in an efficient way, which here means in poly(n) time. By hard-to-reverse, we mean that, for all arguments x, computing $f(x)$ requires poly(n) time, while for all values f of $f(x)$, computing the arguments x and $x + r$ such that $f(x) = f(x + r) = f$ requires exp(n) time.

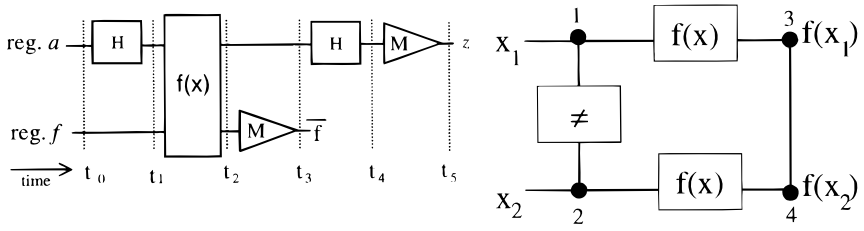
Figure 1a gives the algorithm. H denotes the Hadamard transform (Cleve *et al.*, 1997), the Boolean gate $f(x)$ identically repeats the input x (reg. a) in a corresponding output, and computes $f(x)$ adding it to the former content (0) of register v. M denotes the action of measuring the content of a register. The algorithm proceeds through the following actions:

(a) Prepare $|\varphi, t_0\rangle_{av} = |0\rangle_a|0\rangle_v$.

(b) Perform the H on register a: $|\varphi, t_1\rangle_{av} = (1/\sqrt{N})\ \Sigma_x\ |x\rangle_a|0\rangle_v$ ($N = 2^n$).

(c) Compute $f(x)$, add the result to the former content of register v: $|\varphi, t_2\rangle_{av} = (1/\sqrt{N})\ \Sigma_x\ |x\rangle_a|f(x)\rangle_v$.

(d) Measure [v]: $|\beta, t_3\rangle_{av} = (1/\sqrt{2})(|\bar{x}\rangle_a + |\bar{x} + r\rangle_a)|\bar{f}\rangle_v$. Performing or skipping step (d) is *equivalent*, but assuming it has been performed makes understanding easier. This equivalence can be explained as follows. Let us think of skipping step (d) and measure [a] first, at time t_4. In Fig. 1a, M on v should be shifted at least after t_5. Whether [v] is measured after t_5 is a matter of indifference. Then we can think of measuring it. This induces a "wave function collapse" (a convenient notion here) of the state of register v on some $|\bar{f}\rangle_v$. Since $|\bar{f}\rangle_v$ is disentangled from the state of register a, and no operation is performed on register v after time t_2, backdating collapse at time t_2 (which is legitimate, according to von Neumann and others) means backdating the result of collapse ($|\bar{f}\rangle_v$) as it is. This is equivalent to having performed step (d).



(a) (b)

Fig. 1.

Ekert and Jozsa (1998) have shown that quantum entanglement is essential in providing quantum computation speedup. After measuring $f(x)$, there remains no entanglement. The remaining actions, performed on register a, use interference (which generates no entanglement) to "extract" r out of the superposition $(1/\sqrt{2})(|\bar{x}\rangle_a + |\bar{x} + r\rangle_a)$. We conclude that greater than classical efficiency has already been achieved by reaching $|\beta, t_3\rangle_{av}$. r is "extracted" as follows:

(e) Act with H on a: $|\beta, t_4\rangle_{av} = (1/\sqrt{N})\,\Sigma_z\,(-1)^{\bar{x}\cdot z}[1 + (-1)^{r\cdot z}]|z\rangle_a|\bar{f}\rangle_v$; the dot denotes the module 2 inner product of two numbers in binary notation.

(f) Measure $[a]$ in $|\beta, t_4\rangle_{av}$, obtaining the result z: $r \cdot z$ must be 0 for registered z—see the form of $|\beta, t_4\rangle_{av}$.

(g) By repeating the overall computation a number of times poly(n) on average, a number of constraints $r \cdot z = 0$ sufficient to identify r is gathered.

Let us see how quantum computation speedup is achieved in the time interval $[t_1, t_3]$, involving entanglement creation and disentanglement. In the modified Simon algorithm, the state-before-measurement is the superposition: $|\varphi, t_2\rangle_{av} = (1/\sqrt{N})\,\Sigma_x\,|x\rangle_a|f(x)\rangle_v$, where x ranges over 0, 1, . . . , $N - 1$. Given the character of $f(x)$, the outcome of measuring $[v]$ has the form $|\beta, t_3\rangle_{av} = (1/\sqrt{N})(|\bar{x}\rangle_a + |\bar{x} + r\rangle_a)|\bar{f}\rangle_v$, where $f(\bar{x}) = f(\bar{x} + r) = \bar{f}$. As said before, we assume that efficiency has already been achieved by preparing $|\beta, t_3\rangle_{av}$ which, for short, we can consider to be "the solution."

It can be seen that measuring $[v]$ in $|\varphi, t_2\rangle_{av}$ brings in, through Eqs. (3) and (4), the following constraints on the arguments and values of $f(x)$: $f(x_1) = 3Df(x_2)$, $x_1 \neq x_2$. Since we are dealing with natural numbers, this is a succinct way of representing a *system of simultaneous Boolean equations*. Equation (5) becomes just the specification $f(x_1) = f(x_2) = \bar{f}$. Figure 1b represents this system in network form. The output of gate 1–2 yields the function c: $B^n \times B^n \to B$ defined as follows: $c(x_1, x_2) = 1 - \delta_{x_1,x_2}$, where δ is the Kronecker symbol. In order to have $x_1 \neq x_2$, this output must be constrained to 1. Both gates 1–3 and 2–4 transform an input x into the output $f(x)$. We should keep in mind that the network shown in Fig. 1b is just the representation of a system of simultaneous Boolean equations: time is not involved [just like in Eqs. (3)–(5)], thus inputs and outputs lose any time-related meaning: they just stand for the arguments and the values of a function.

On one hand, since $f(x)$ is hard-to-reverse, the Boolean network of Fig. 1b is hard to satisfy by classical means. As can be seen, finding a valuation of x_1 and x_2 which satisfies the network implies reversing $f(x)$ at least once, given that gates 1–3 and 2–4 belong to a loop. This operation takes exp(n) time by assumption. On the other hand, once $|\varphi, t_2\rangle$ has been prepared, the network, no matter what its computational complexity, is concurrently created and solved by the action of measuring $[v]$. A solution, a proper valuation of

x_1 and x_2, is represented in the quantum superposition $|\beta, t_3\rangle_{av}$ (r can "easily" be extracted from this superposition). Since $|\varphi, t_2\rangle_{av}$ is prepared in poly(n) time, there is an exponential speedup. In the case of Simon's algorithm, given proper initial actions, quantum measurement can be seen as an *analog form of computation*, capable of satisfying a system of simultaneous Boolean equations in one shot.

ACKNOWLEDGMENTS

Thanks are due to T. Beth, A. Ekert, D. Finkelstein, and V. Vedral for stimulating discussions and valuable comments.

REFERENCES

G. Castagnoli (1995), *Int. J. Theor. Phys.*, **34**, 1283.
G. Castagnoli (1998), *Physica D* **120**, 48.
G. Castagnoli and D. Monti (1998), Quantum computation based on particle statistics, *Chaos Solitons Fractals*, to appear.
J. G. Cramer, *Rev. Mod. Phys.* **58**, 647 (1986).
R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca (1997), Quantum algorithms revisited, *Proc. R. Soc. Lond. A*, to appear.
A. Ekert and R. Jozsa (1998), Quantum algorithm: entanglement enhanced information processing, *Phil. Trans. R. Soc.* (*Lond.*), to appear.
D. Finkelstein (1996), *Quantum Relativity*, Springer, Berlin.
P. Shor (1994), in *Proceedings of the 35th Annual Symposium on the Foundation of Computer Science, Los Alamitos, California*, p. 124.
D. R. Simon (1994), in *Proceedings of the 35th Annual Symposium on the Foundation of Computer Science*, Santa Fe, New Mexico.